REMARKS

1. Posture of the case. This is a reply to the first Office action in the case.

The drawings stand objected to due to informalities.

Claims 2-7 stand rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. This is because claim 2 refers to steps a), b) and c) in claim 1, but the original claim 1 did not include "a)," "b)," and "c)."

Claims 1-28 stand rejected under 35 USC 102 as being anticipated by U.S. Patent No. 6,266,692 ("Greenstein") and also as being anticipated by European Patent Application No. EP0946022A2 ("Haruhisa").

2. Drawings. Formal Drawings are herein submitted under separate cover addressed to the Official Draftsman as requested in the Office Action.

3. Claim rejections under 35 USC 112, second paragraph.

Claim 1 has been amended to include step identifiers "a)," "b)," and "c)" to overcome the rejection.

4. Claim rejections under 35 USC 102.

Independent claims 1, 8, 15 and 22 are herein amended to overcome the rejections. According to amended claim 1, electronic messages that are screened have respective reply addresses for senders and addresses for respective designated receivers. (All the steps set out in claim 1 are performed by a screening agent for the designated receiver.) The screening agent determines whether one such as these electronic messages includes a pass that was generated by the screening agent from an earlier-received version of the electronic message and forwards the message to the receiver if it does have the pass. If the message does not have the pass, the agent generates a notice and a pass for the sender. The notice includes information making the pass available to the sender and requesting the sender to return the pass to an indicated address. (The pass could be "made available," for example, by sending the notice to the sender in a reply to the message, or by posting it on a web page, etc., as set out in ones of the dependent claims.) The pass is particularized for the sender by the screening agent including in the pass an encrypted version of the sender's address received in the sender's message. The aforementioned determination of whether one of the electronic messages includes a pass involves decrypting a

Docket AUS920000492US1

Appl. No.: 09/666,274
Filed: 09/21/2000

pass associated with the electronic message and determining if the sender's address indicated in the message matches an encrypted address in the pass. Independent claims 8, 15 and 22 have similar language for their respective forms of the invention.

Note that the claimed arrangement is advantageous because the screening agent encrypted the pass, the agent can tell if the pass was generated by the screening agent itself by successfully decrypting the pass. And since the pass included the encrypted address of the sender and was made available to the sender, the screening agent can check for such a pass in any received message and tell if the sender actually received and returned the pass by comparing the sender's address to the encrypted address in the pass.

Claims 2-5, 9-12, 16-19 and 23-26 are amended to conform to the amendments of claims 1, 8, 15 and 22.

Support for amendments. No new matter is added by these amendments, since the original specification and drawings included support for the amendments. See, e.g., page 7, line 16 - page 8, line 7 and FIG. 7 (regarding electronic messages respectively having reply addresses 705 for senders and addresses 710 for designated receivers); page 6, line 16 - page 7, line 11 and FIG. 2 (regarding the point that a screening agent 160 does the steps of determining about passes 230, forwarding messages 240 and generating notices and passes 250, as set out in claim 1, for example); see FIG' s1, 7 and 8 (regarding looking for a pass in message 150.1 generated by the screening agent from an earlier-received version 130.1 of the electronic message 150.1); page 6, line 16 - page 7, line 11 and FIG. 2 (regarding the forwarding 240 of the electronic message to the receiver being done responsive to a message having such a pass that was generated by the screening agent from the earlier-received version of the electronic message); see FIG. 7 (regarding making the pass available to the sender, which in the illustrated example is by reply message 140.1); see FIG. 7 (regarding the pass being particularized for the sender by including in the pass 730 an encrypted version of the sender's address 705 received in the message 130.1); and see FIG. 8 (regarding step a) including a step of determining whether such a one of the electronic messages has such a pass 730, how the encrypted address of the pass includes an indicated sender 820 and how this matches the message's sender address 805).

The elements, steps and limitations of the amended, independent claims are not taught or suggested by the cited references.

Docket AUS920000492US1

Appl. No.: 09/666,274
Filed: 09/21/2000

Haruhisa. With regard to Haruhisa, different parts of the process of Haruhisa are done by different organizations. Haruhisa, column 28, paragraph 0147. In contrast, according to the present invention, as claimed in the amended claim 1, for example, the steps are all performed by a single screening agent for the receiver of the electronic message. (Claims 8, 15 and 22 have similar language.)

Also, the Office action compares step c) in claim 1 to the authentication step 1435 of Haruhisa. However, the authentication step of Haruhisa is not done in response to an e-mail message not having a pass, as claimed. Haruhisa is vague about this authentication. It appears from the context that this vagueness is because the authentication step 1435 refers to a well-known process, which is quite different than the process of step c) in the present application, claim 1. According to the well-known authentication process, in order to verify a signature on a document a receiver (i.e., the secure communications service ("SCS") referred to by Haruhisa) uses a certification authority's ("CA's") public key to check the signature on a certificate of the sender. (Successful de-encryption of the certificate proves that the CA created it. After the certificate is de-encrypted, the SCS can check the sender's status with the CA and confirm that the certificate information concerning the sender's identity has not been altered.) According to this well-known process, in the context of signature authentication taught by Haruhisa, step 1435 no doubt may include the SCS then taking the sender's public key from the certificate and using it to check the sender's signature. If the sender's public key successfully de-encrypts the sender's signature, then since the CA has certified the matching public key, the SCS is assured that the sender's purported signature was actually created using the sender's private key. Consequently, the SCS is assured the signature is authentic. This authentication is not something done in response to the sender's e-mail not having a pass, as is the case for step c) of claim 1 in the present case. (Claims 8, 15 and 22 have similar language.)

Moreover, the independent claims in the present application have been amended to clarify these and other distinctions. In particular, the claim as amended makes it clear that the authentication step 1435 of Haruhisa is not like step c) in claim 1 because the authentication step does not involve a screening agent generating a notice to a sender to return a pass also generated by the screening agent, where the sending of the notice is responsive to that same screening agent

Docket AUS920000492US1

Appl. No.: 09/666,274
Filed: 09/21/2000

for the designated receiver determining that a message from the sender to the sender does not have the pass.

The amendments submitted herein clarify important differences between Applicant's invention and the teachings of Haruhisa. In general, the teachings of Haruhisa are quite different than that of the present claimed invention. Haruhisa is concerned with enabling secure communication while maintaining anonymity of sender and receiver. Haruhisa requires senders and receivers to go through a registration process with both a certification authority and an anonymous directory service. The present invention does not require this third and fourth party registration and does not concern maintaining anonymity. Confusion over this point concerning anonymity may have arisen due to the statement in the Summary of the Invention in the present application which states that "pass generation and sender notification may be without regard for the identity of the sender." Page 2, lines 17-18. However, this statement is merely making the point that identity of the sender may be immaterial to the method and structure of the invention from the standpoint of generating a pass and notifying the sender. It does not suggest that anonymity is necessarily an objective of the present invention.

Greenstein. With regard to Greenstein, there is a teaching therein that a "passcode" must be included in an e-mail header in order for a recipient to accept the mail. In the present invention a pass is generated and made available to a sender by the screening agent responsive to a message from the sender that is without a pass. And the screening agent looks for this pass in association with another message from the sender (which may be the same message, returned again by the sender, but this time including the pass). In an embodiment of the present invention, this pass must be sent back to the recipient in a header of the sender's message. Superficially it may appear that sending a pass in a header of a sender's message is a similar concept to the teaching of Greenstein that a certain passcode must be included in an e-mail header. However, there are important differences. First, even with respect to the originally submitted claims, Greenstein does not teach that a pass is generated to a sender responsive to a message from the sender that is without a pass. The cited passage of Greenstein relied upon by the Office action merely teaches that a receiver's passcode may be provide to a sender for inclusion in the sender's e-mail header. This does not indicate that the passcode is sent responsive to a message from the sender that is without a pass.

Moreover, the amendments submitted herein clarify important differences between Applicant's invention and the teachings of Greenstein. In important respects the pass of the present invention is not the same as the passcode taught by Greenstein. As stated in amended claim 1, "the pass is particularized for the sender by including in the pass an encrypted version of the sender's address received in the message." Also, the amended claim states that "step a) includes determining whether such a one of the electronic messages has such a pass and whether the encrypted address of the pass matches the message's sender address." Greenstein does not teach or suggest this.

For the above reasons Applicant contends claims 1, 8, 15, and 22 are allowable. Claims 2-5, 9-12, 16-19 and 23-26 are allowable at least because they depend upon respective independent claims 1, 8, 15, and 22.
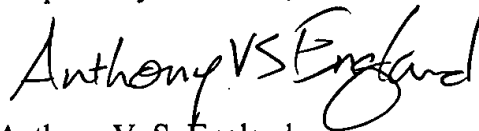
PRIOR ART OF RECORD

Applicant has reviewed the prior art of record cited by but not relied upon by Examiner, and asserts that the invention is patentably distinct.

REQUESTED ACTION

Applicant contends that the invention as claimed in accordance with amendments submitted herein is patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,

Anthony VS England

Anthony V. S. England
Attorney for Applicants
Registration No. 35,129
512-477-7165
a@aengland.com